

AMENDMENTS

In the Claims

Claims 3, 4, 6-12, 15-22, 25 and 27-30 were pending at the time of the Office Action.

Claims 3, 4, 6-12, 15-17, 25 and 27-30 are expressly allowed.

Claims 18 and 21 are rejected.

Claims 19, 20, and 22 are objected to.

Claims 19, 21 and 22 are amended by the current response.

Claim 18 is canceled by the current response.

Accordingly, claims 3, 4, 6-12, 15-17, 19-22, 25 and 27-30 remain pending.

Please amend claims 19, 21, and 22 as indicated in the following complete listing of claims.

Listing of Claims:

1-2. (Canceled)

3. (Previously presented) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

generating a seed value;

producing a hash seed value based on the seed value using a one-way hash function;

1 generating an application storage key from the hash seed value;
2 encrypting the information using the application storage key; and
3 associating the access predicate with the encrypted information.
4

5 4. (Previously presented) A computerized method for key-based
6 secure storage comprising:

7 downloading information and an access predicate that specifies
8 requirements for an application to access the information;

9 generating a seed value;

10 producing a first hash seed value based on the seed value using a one-way
11 hash function;

12 producing a second hash seed value based on the seed value and a user
13 identifier using a keyed hash function;

14 generating a user storage key from the second hash seed value;

15 encrypting the information using the user storage key; and

16 associating the access predicate with the encrypted information.
17

18 5. (Canceled)
19

20 6. (Previously presented) A computerized method for key-based
21 secure storage comprising:

22 downloading information and an access predicate that specifies
23 requirements for an application to access the information;

24 obtaining a storage key;

25 encrypting the information using the storage key;

1 associating the access predicate with the encrypted information;
2 obtaining an operating system storage key;
3 encrypting the access predicate with the operating system storage key; and
4 encrypting a plurality of other storage keys using the operating system
5 storage key, wherein the other storage keys are selected from the group consisting
6 of application storage keys and user storage keys.

7
8 7. (Previously presented) A computerized method for key-based
9 secure storage comprising:

10 downloading information and an access predicate that specifies
11 requirements for an application to access the information;

12 obtaining a storage key;

13 encrypting the information using the storage key;

14 associating the access predicate with the encrypted information;

15 generating a seed value;

16 generating an operating system storage key based on the seed value; and

17 encrypting the access predicate with the operating system storage key.

18
19 8. (Previously presented) A computerized method for key-based
20 secure storage comprising:

21 downloading information and an access predicate that specifies
22 requirements for an application to access the information;

23 generating a seed value for the application;

24 producing an application hash seed value based on the seed value for the
25 application using an application-specific one-way hash function;

1 generating an application storage key from the application hash seed value;
2 generating a seed value for a user;
3 producing a first user hash seed value based on the seed value for the user
4 using a one-way hash function;
5 producing a second user hash seed value based on the first user hash seed
6 value and a user identifier using a keyed hash function;
7 generating a user storage key from the second user hash seed value, the
8 application storage key and the user storage key to encrypt information containing
9 a portion specific to an application and a portion specific to the user;
10 encrypting the information using the application storage key and the user
11 storage key; and
12 associating the access predicate with the encrypted information.

13
14 9. (Previously presented) A computerized method for key-based
15 secure storage comprising:

16 downloading information and an access predicate that specifies
17 requirements for an application to access the information;
18 obtaining a storage key;
19 encrypting the information using the storage key;
20 associating the access predicate with the encrypted information;
21 storing the storage key in a key vault provided by a third-party; and
22 recovering the storage key from the key vault.

23
24 10. (Original) The computerized method of claim 9, wherein
25 recovering the storage key comprises:

1 requesting recovery of the storage key; and
2 providing information to the third-party to enable validation of the request.
3

4 11. (Previously presented) The computerized method of claim 9,
5 further comprising:

6 selecting the key vault from a plurality of key vaults provided by a trusted
7 operating system.
8

9 12. (Previously presented) The computerized method of claim 9,
10 further comprising:

11 selecting the key vault designated by a provider of the information.
12

13 13-14. (Canceled)
14

15 15. (Previously presented) A computer system comprising:

16 a processing unit;

17 a system memory coupled to the processing unit through a system bus;

18 a computer-readable medium coupled to the processing unit through a
19 system bus;

20 a generate key function executed from the computer-readable medium by
21 the processing unit, wherein the generate key function causes the processing unit
22 to generate an operating system storage key based on an identity for the operating
23 system and based on a seed.
24
25

1 16. (Previously presented) A computer system comprising:
2 a processing unit;
3 a system memory coupled to the processing unit through a system bus;
4 a computer-readable medium coupled to the processing unit through a
5 system bus;
6 a generate key function executed from the computer-readable medium by
7 the processing unit, wherein the generate key function causes the processing unit
8 to generate an operating system storage key based on an identity for the operating
9 system;
10 an application specific one-way hash function executed from the
11 computer-readable medium by the processing unit, wherein the application
12 specific one-way hash function causes the processing unit to generate an
13 application storage key from a hashed seed; and
14 a generate application key function executed from the computer-readable
15 medium by the processing unit, wherein the generate application key function
16 causes the processing unit to generate the hashed seed from an application seed.

17
18 17. (Previously presented) A computer system comprising:
19 a processing unit;
20 a system memory coupled to the processing unit through a system bus;
21 a computer-readable medium coupled to the processing unit through a
22 system bus;
23 a generate key function executed from the computer-readable medium by
24 the processing unit, wherein the generate key function causes the processing unit
25

1 to generate an operating system storage key based on an identity for the operating
2 system;

3 a key-hash function executed from the computer-readable medium by the
4 processing unit, wherein the key-hash function causes the processing unit to
5 generate a user storage key from a hashed seed and an identity for the user;

6 a one-way hash function executed from the computer-readable medium by
7 the processing unit, wherein the one-way hash function causes the processing unit
8 to generate the hashed seed from a previously hashed seed; and

9 a generate user key function executed from the computer-readable medium
10 by the processing unit, wherein the generate user key function causes the
11 processing unit to generate the previously hashed seed from a user seed.

12
13 18. (Canceled)

14
15 19. (Currently amended) A computer system comprising:

16 a processing unit;

17 a system memory coupled to the processing unit through a system bus;

18 a computer-readable medium coupled to the processing unit through a
19 system bus; and

20 a trusted operating system executed from the computer-readable medium by
21 the processing unit, wherein the trusted operating system causes the processing
22 unit to encrypt downloaded information using a storage key based on a seed value.

23 ~~The computer system of claim 18, wherein the trusted operating system further~~
24 ~~causes the processing unit to encrypt an access predicate associated with the~~
25 ~~downloaded information using an operating system storage key, to encrypt the~~

1 seed value for the storage key using the operating system storage key, and to
2 associate the encrypted access predicate with the encrypted seed value.

3
4 20. (Previously presented) The computer system of claim 19,
5 wherein the trusted operating system further causes the processing unit to validate
6 each application requesting access to the downloaded information using the access
7 predicate, and decrypts the seed value for use by a validated application.

8
9 21. (Currently amended) The computer system of claim 19 18,
10 wherein the storage key used to encrypt the downloaded information is specific to
11 an application.

12
13 22. (Currently amended) A computer system comprising:
14 a processing unit;
15 a system memory coupled to the processing unit through a system bus;
16 a computer-readable medium coupled to the processing unit through a
17 system bus; and
18 a trusted operating system executed from the computer-readable medium by
19 the processing unit, wherein the trusted operating system causes the processing
20 unit to encrypt downloaded information using a storage key based on a seed value,
21 and ~~The computer system of claim 18,~~ wherein the storage key used to encrypt the
22 downloaded information is specific to a user.

23
24 23-24. (Canceled)

1 25. (Previously presented) A computerized method for key-based
2 secure storage comprising:

3 downloading information and an access predicate that specifies
4 requirements for an application to access the information;

5 obtaining a storage key;

6 encrypting the information using the storage key;

7 associating the access predicate with the encrypted information;

8 storing the storage key in a key vault provided by a third-party;

9 recovering the storage key from the key vault; and

10 selecting the key vault from a plurality of key vaults provided by an
11 authenticated operating system.

12
13 26. (Canceled)

14
15 27. (Previously presented) A computer system comprising:

16 a processing unit;

17 a system memory coupled to the processing unit through a system bus;

18 a computer-readable medium coupled to the processing unit through a
19 system bus; and

20 an authenticated operating system configured to execute on the processing
21 unit from the computer-readable medium, the authenticated operating system
22 causing the processing unit to encrypt downloaded information using a storage key
23 based on a seed value;

24 wherein the authenticated operating system further causes the processing
25 unit to encrypt an access predicate associated with the downloaded information

1 using an operating system storage key, to encrypt the seed value for the storage
2 key using the operating system storage key, and to associate the encrypted access
3 predicate with the encrypted seed value.
4

5 28. (Previously presented) The computer system of claim 27, wherein
6 the authenticated operating system further causes the processing unit to validate
7 each application requesting access to the downloaded information using the access
8 predicate, and decrypts the seed value for use by a validated application.
9

10 29. (Previously presented) The computer system of claim 27, wherein
11 the storage key used to encrypt the downloaded information is specific to an
12 application.
13

14 30. (Previously presented) The computer system of claim 27, wherein
15 the storage key used to encrypt the downloaded information is specific to a user.
16
17
18
19
20
21
22
23
24
25